center, according to the public-key method. The combination of England, Davis and Wong does not disclose of suggest the claimed method.

As discussed in the interview, the Office Action recognizes that England does not disclose or suggest generating a certificate using a public key and a secret key and instead relies on the disclosure of Davis.[1] For at least the reasons set forth below, it is respectfully submitted that Davis does not remedy the deficiencies of England with respect to Applicant's claims, and the inconsistent interpretation of England employed by the Patent Office in support of the rejection is improper.

THE DISCLOSURE OF ENGLAND

As discussed in the interview, England discloses a digital rights management operating system involving a number of certificates including a manufacturer certificate 166, CPU certificate 202, and rights manager certificate 210. England does not disclose or suggest that any of these certificates are generated in the manner required by Applicant's claim 1. Specifically, England fails to disclose or suggest ***a public key of a software signature site*** and ***a secret key of a control entity of a trust center***. Accordingly, England does not disclose or suggest generating a software signature certificate in the manner required by Applicant's claim 1. The Office Action, however, continues to rely on England for the disclosure of the above-identified features to support the obviousness rejection.

[1] Page 6, Office Action.

THE OFFICE ACTION'S CITATIONS TO ENGLAND

As mentioned above, the Office Action recognizes that England does not disclose or suggest generating a software signature certificate including a public and private key and thus, does not cite to England for the disclosure of the above-identified features elements of claim 1 in the rejection section of the Office Action. In the Response to Arguments section of the Office Action, England is cited for the disclosure of a software signature site, a public key of the software signature site, and a secret key of a trust control entity of a trust center.

The Response to Arguments section cites column 7, line 63 – column 8, line 14 of England for the disclosure of a software signature site and a ***public key*** of the software signature site. The Office Action states that this section discloses that the manufacturer has a public/private key pair and that the "particular ***private key*** is used to sign the software."[2] First, Applicant respectfully submits that the disclosure of a ***private key*** does not disclose or suggest a ***public key*** or use of a public key of a software signature site for generating a software signature certificate. Second, as previously argued this section does not mention generating a ***software signature certificate***. Rather, this section is directed to producing certificate 166 testifying that a ***CPU*** was produced according to a known specification. Further, England discloses that the pair of public and private keys are unique to the CPU.[3] Thus, even if it were assumed that the manufacturer of the CPU is a software developer and includes

[2] Emphasis added.
[3] Column 7, lines 51-52.

a CPU public key, one of ordinary skill in the art would not view the disclosure of CPU certification as certification of the software.

As further discussed in the interview, the Office Action's interpretation of England in the Response to Arguments section is inconsistent with the rejection of claim 1. The Office Action relies upon column 11, lines 54 – 59 of England for the disclosure of checking signed software integrity using a public key. This section of England discloses a rights manager certificate for loaded components of the digital right management operating system (DRMOS). England, however, does not disclose or suggest that a DRMOS certificate is related to the CPU certificate. Because it is improper to take inconsistent positions in interpreting a reference to reject an independent claim, the interpretation in the Response to Arguments section cannot support the rejection.

The Response to Arguments section cites column 8, line 66 – column 9, line 3 of England for the alleged disclosure of a secret key of a control entity of a trust center and alleges that England discloses a "third party key is used to sign software." The cited portion of England, however, does not mention a third party key. As previously argued, this cited portion of England discloses that "operating system-level components [*are*] digitally signed by their developers or a trusted third party". Notably absent from this or any other portion of England is any disclosure or suggestion of ***a secret key*** of a control entity of a trust center. Further, England does not disclose or suggest any relationship between the "third party" and manufacturer certificate 166. Even if it were assumed that a CPU manufacturer is, "a control entity of a trust center," England discloses that

certificate 166 includes the ***public key*** of the CPU, K_{CPU}, and ***not*** the private key K_{CPU}^{-1}. Accordingly, England does not disclose or suggest a secret key of a control entity of a trust center. Nor for that matter does England disclose generating a certificate using a secret key of a trust center as recited in Applicant's claim 1.

The Disclosure of Davis

Davis discloses a method for implementing a key pair and digital certificate into a semiconductor device.[4] Although Davis discloses a key pair, Davis does not disclose or suggest that the key pair relates to a ***public key*** of a software signature site and a ***secret key*** of a control entity of a trust center. In contrast to the method recited in Applicant's claim 1, Davis discloses a random number generator to generate key pairs.[5]

The Office Action's Citation's to Davis

As discussed in the interview, the Office Action cites column 5, lines 43-59 of Davis for the disclosure of generating a signature certificate using the public key of the signature site and a secret key of a control entity, according to a public key method. This section discloses signing a public key of a hardware device with a manufacturer's private key for a hardware device. Like England, Davis does not disclose or suggest that the public key is associated with a software signature site. Moreover, Davis fails to disclose or suggest that the manufacturer key is associated with a control entity of a trust center.

[4] Abstract.
[5] Column 5, lines 31-33.

In the Response to Arguments section of the Office Action, the Patent Office merely reiterates the arguments in the rejection and fails to address Applicant's previously submitted arguments.

Accordingly, Davis does not remedy the deficiencies of England.

As previously argued, Wong does not disclose generating a software signature certificate and thus, does not remedy the deficiencies of Applicant's claim 1. Applicant respectfully submits that the combination of England, Davis and Wong does not disclose or suggest generating a software signature certificate as required by claim 1.

Claims 3-6 and 8-18 are patentably distinguishable over the combination of England, Davis and Wong at least by virtue of dependency from claim 1.

Independent claim 7 recites a method involving a software signature certificate, and is patentably distinguishable over the combination of England, Davis and Wong for similar reasons to those discussed above with respect to claim 1.

Regarding Applicant's independent claim 19, the Office Action cites column 11, lines 54-59 of England for checking if the software signature certificate has been changed or manipulated. As previously argued, a disclosure of checking a signature, based solely on signature validity, does not, however, disclose or suggest checking a software signature certificate for change or manipulation as recited in claim 19. The Response to Arguments section, however, does not address Applicant's arguments. Applicant respectfully requests that Patent Office address Applicant's arguments if the rejection is to

be maintained. Neither Davis nor Wong remedy the deficiencies of England with respect to claim 19. Claim 20 is patentably distinguishable over the combination of England, Davis and Wong at least by virtue of its dependency from claim 19.

If there are any questions regarding this response or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323 (Docket # 080437.53236US).

Respectfully submitted,

April 15, 2010

/Stephen W. Palan, Reg. # 43,420/
Stephen W. Palan
Registration No. 43,420

CROWELL & MORING, LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
SWP:crr